Pôle Universitaire Léonard de Vinci
ESI GI 3906 – Cryptography

Semester 9 – Year 2008-2009
ESILV – Class of 2009

Final Exam

Solutions

Problem I

1.

a . This is a self-signed certificate since the issuer and the subject have the same distinguished name

b .
Issued to: Visa eCommerce Root (common name)
Signed by: Visa eCommerce Root (common name)

c . Valid until Jun 24 2022 00:16:12 (note that the seconds are present)

d . This certificate uses RSA as the primary signature algorithm, combine with the Secure Hash Standard SHA. The signature is obtained by computing the SHA-1 value of the tbsCertificate part. The hashed value is then encrypted with the private RSA key (not published here). The resulting signature is then attached (along with the signature algorithm descriptor) to the certificate, as indicated by the ASN.1 description.

e . This certificate contains a RSA public key

- the modulus is 2048 bits wide
- the exponent is 65537

A 2048 bits modulus is considered to be safe by today's standard.

2.

a . The ACME certificate will be a public key certificate. It will be signed by "Visa eCommerce Root". The distinguished names are as follow:

```
Signer (Signed by): C=US, O=VISA, OU=Visa International Service Association,
                    CN=Visa eCommerce Root
Signee (Issued to): C=US, O=ACME, OU=ACME Internation Company, CN=store.acme.com
```

The Country (C) and Organization Unit (OU) can be anything - The most important part is the common name (CN) which is defined here with the server fully qualified name.

b . No. You will be able to create a certificate request - but you will not be able to sign it. Only the signer can issue the certificate.

c . It is a bad idea for 2 reasons:

- 50 years will bring around year 2058 which goes well beyond the signer certificate valid year (2022)
- The computation will be susceptible to the year 2038 bug

d . You can do the verification is two ways:

- With a browser, the certificate can be loaded and verified
- Manually, with OpenSSL, you can dump its content (command x509) and look for the field of you interest.

In both cases, the common name must be verified as well as the signer distinguished name. Finally, attention should be paid to the validity period. The certificate signature can also be recomputed and verified. The exact nature of this operation will depend on the chosen signature algorithm.

Problem II

1. Let $y \in [\![1, 52]\!]$. Let (q, r) be the Euclidean division and the Euclidean of y by 13 (*i.e.* $y = 13q + r$.) We have $q \in \{0, 1, 2, 3\}$ and $r \in [\![1, 13]\!]$. If $q = 0$ let $s = Spades$, if $q = 1$ let $s = Hearts$, if $q = 2$ let $s = Diamonds$, if $q = 3$ let $s = Clubs$. Let $n = f_N^{-1}(r)$. We have

$$y = f(s, n)$$

This proves that f is onto (surjective).

Let (s, n) and (s', n') be two elements in D such that $f(s, n) = f(s', n')$. Let (q, r) be the Euclidean division and the Euclidean of y by 13. We have $f_N(n') = f_N(n) = r$. Since f_N is into, we have $n = n'$. We have $f_S(s') = f_S(s) = q$. Since f_S is into, we have $s = s'$. Consequently, $(s, n) = (s', n')$. Thus, f is into (injective).

As a consequence f is one-to-one (bijective).

2. Let y be the number to be decrypted. Following the first question, let (q, r) be the Euclidean division and the Euclidean of y by 13. We have $q \in \{0, 1, 2, 3\}$ and $r \in [\![1, 13]\!]$. If $q = 0$ let $s = Spades$, if $q = 1$ let $s = Hearts$, if $q = 2$ let $s = Diamonds$, if $q = 3$ let $s = Clubs$. Let $n = f_N^{-1}(r)$.

3. There are $\binom{5}{52} = 2,598,960$ possible hands. Therefore, the probability to have one specific hand is

$$\frac{1}{2,598,960}$$

The probability that this happens 20 times in a row is

$$\left(\frac{1}{2,598,960}\right)^{20} \simeq (4\ 10^{-7})^{20} = 2^{40}10^{-140} \simeq= 10^{12}10^{-140} \simeq 10^{-128}$$

4. Mallaury could be cheating (and is very likely cheating considering the odds indicated in the previous questions).

The public key algorithm (RSA) that is being used does not randomize the encrypted messages. Mallaury can simply encode all of the cards with the public keys of Alice, Bob and her own (in the right order), then compare the results with what she has and choose the cards she wants.

5. In steps 3, 4 and 5, some random data should be added to the number representing the card (in a way that the card number can be identified). For instance, One could add a random number R multiplied by 53 to get the card number C, one will simply compute the $53 \times R + C$ modulo 53 to recover C. If the random data is long enough (thus there are too many of them), it will ensure that Mallaury cannot encrypt all possible numbers and random data.

Problem III

1. Let $n = 4099$, $s = 2$ and $d = 2049$, we have

$$n - 1 = 2^r d$$

For a thousand different a

i) $a^d \equiv 1 \pmod{n}$

ii) $a^{2^r d} \equiv -1 \pmod{n}$ for a given r between 0 and $s - 1$

thus the Miller-Rabin test yields that n is a prime number. The probability of a false positive is

$$4^{-1000} = 2^{-2000}$$

2. Alice computes

$$g^a \bmod p = 4^2 = 2^4$$

and sends this number to Bob, who computes

$$(g^a \bmod p)^3 \bmod p = (2^4)^3 = 2^{12} = 4096$$

Consequently, the shared secret of Alice and Bob is 4096.

3. We could not have chosen $p = 4100$ in the previous question because 4100 is not a prime number.